CLAIMS

1. A method of capturing a security breach, comprising:
deploying a honey pot;
detecting a breach of the honey pot; and
automatically redeploying the honey pot.

2. The method of claim 1, further including analyzing the breach.

3. The method of claim 1, further including automatically analyzing the breach.

4. The method of claim 1, wherein the breach is automatically detected.

5. The method of claim 1, further including copying state information from the honey pot.

6. The method of claim 1, further including shutting down the honey pot.

7. The method of claim 1, further including configuring the honey pot.

8. The method of claim 1, further including copying a honey pot image.

9. The method of claim 1, wherein the honey pot is a physical machine.

10. The method of claim 1, wherein the honey pot is a virtual machine.

11. The method of claim 1, wherein the honey pot is a VMware virtual machine.

12. The method of claim 1, wherein the honey pot is a Microsoft Virtual PC virtual machine.

13. The method of claim 1, wherein detecting is based on the number of outgoing connections detected.

14. The method of claim 1, wherein detecting is based on the number of incoming connections detected.

15. The method of claim 1, wherein detecting is based on an elapsed time.

16. The method of claim 1, wherein the honey pot runs a Windows operating system.

17. The method of claim 1, wherein the honey pot runs a Linux operating system.

18. The method of claim 1, further including saving state information associated with the honey pot.

19. The method of claim 1, further including saving state information associated with the honey pot and wherein saving and redeploying occur in parallel.

20. The method of claim 1, further including analyzing the breach and wherein analyzing and redeploying occur in parallel.

21. The method of claim 1, further including:

receiving an incoming connection associated with an IP address;

mapping the IP address to the honey pot; and

releasing the IP address mapping.

22. The method of claim 1, further including:

receiving an incoming connection associated with an IP address;

mapping the IP address to the honey pot;

releasing the IP address mapping; and

mapping another IP address to the honey pot.

23. A computer program product for capturing a security breach, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

deploying a honey pot;

detecting a breach of the honey pot; and

automatically redeploying the honey pot.

24. A system for capturing a security breach, comprising:

a processor configured to:

deploy a honey pot;

detect a breach of the honey pot; and

automatically redeploy the honey pot; and

a memory coupled with the processor, wherein the memory provides the processor with instructions.